IT Guard

DISTRIBUTION OF LEADING INFORMATION
SECURITY TECHNOLOGIES

PAN – общая информация

Palo Alto Networks – является производителем ключевого элемента инфраструктуры сетевой безопасности и лидером в сегменте NGFW

** 4 раза в «лидерах» в квадрантах Gartner*

paloalto NETWORKS

the network security company™

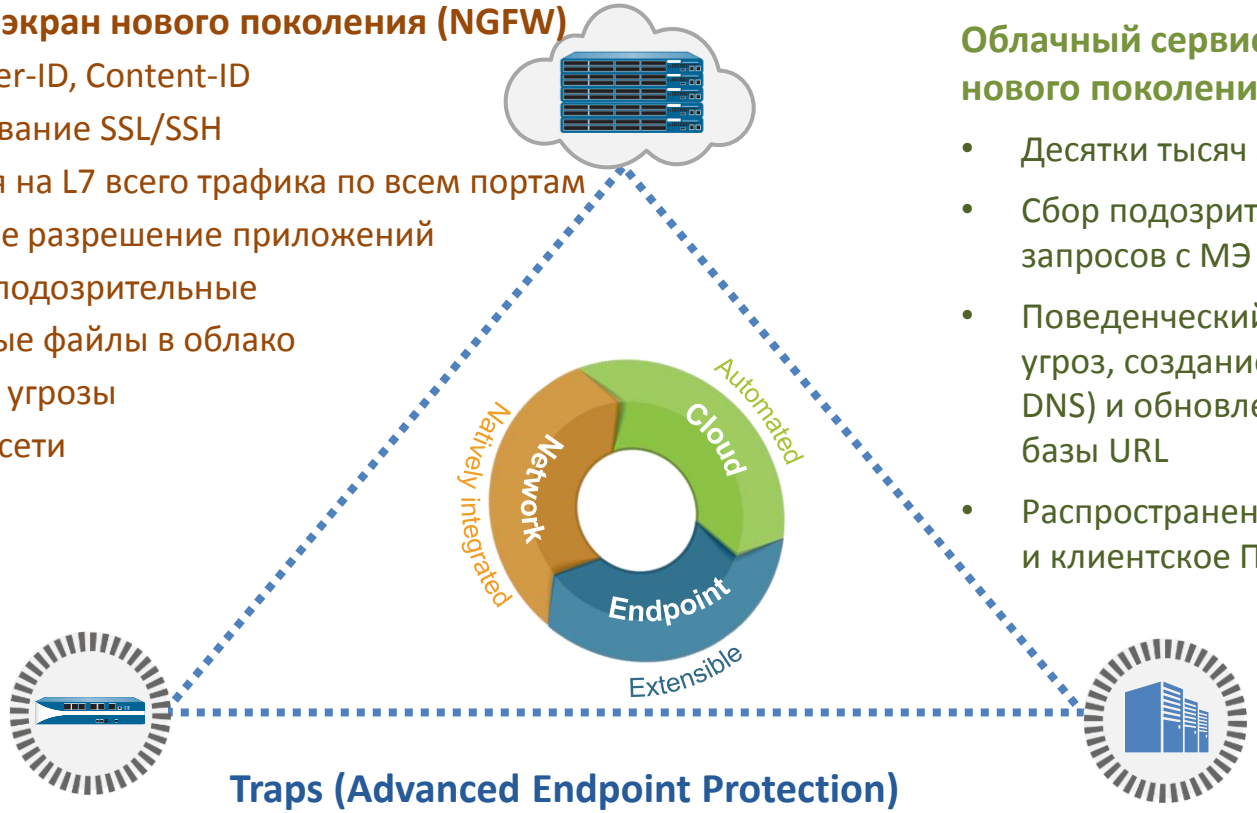
- Инновационные технологии: **App-ID™, User-ID™, Content-ID™, WildFire™**
- 10 000+ корпоративных заказчиков в 100+ странах мира, 40+ из которых внедрили решение стоимостью более $1 000 000
- 50+ текущих крупнейших корпоративных заказчиков в России

РЖД МТС Ростелеком МЧС России EMERCOM

Платформа кибер-безопасности нового поколения

Межсетевой экран нового поколения (NGFW)

- App-ID, User-ID, Content-ID
- Расшифрование SSL/SSH
- Инспекция на L7 всего трафика по всем портам
- Безопасное разрешение приложений
- Отсылает подозрительные неизвестные файлы в облако
- Блокирует угрозы на уровне сети



Облачный сервис защиты от угроз нового поколения (Wildire)

- Десятки тысяч заказчиков
- Сбор подозрительных файлов и DNS-запросов с МЭ и сетевых хостов
- Поведенческий анализ и корреляция угроз, создание сигнатур (IPS, AV, DNS) и обновление репутационной базы URL
- Распространение обновлений на МЭ и клиентское ПО

Traps (Advanced Endpoint Protection)

- Инспекция всех процессов Windows
- Предотвращение известных и неизвестных угроз
- Защита физических и виртуальных сред и мобильных ПК
- Интеграция с облачной защитой от угроз

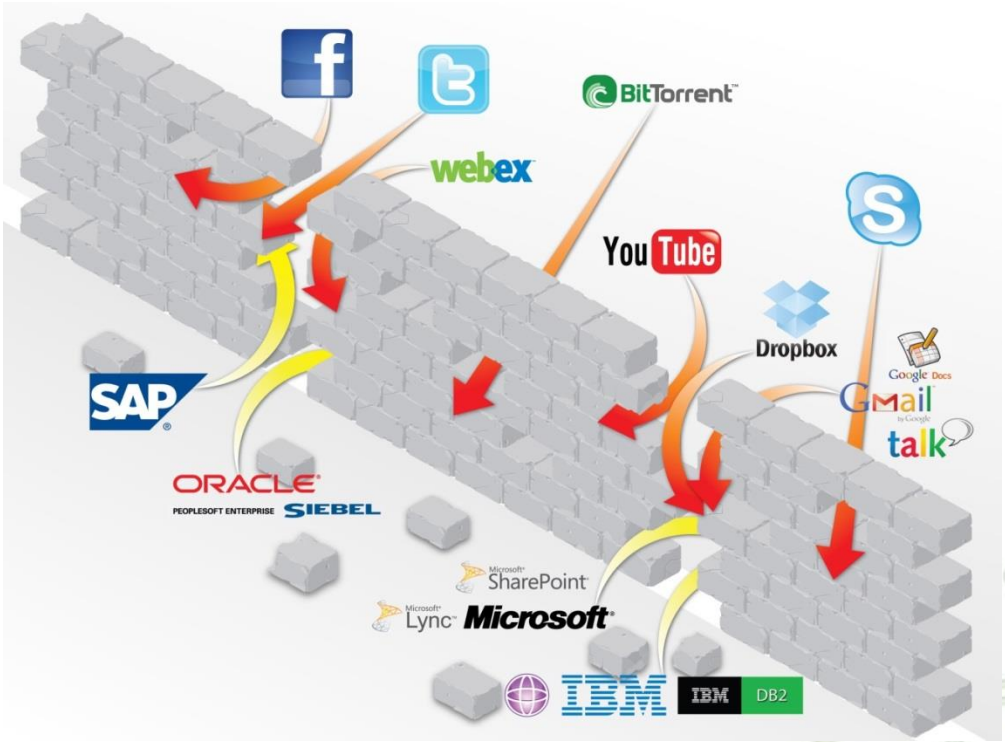
PAN: механизмы защиты

Политики межсетевых экранов базируются на контроле:

- Портов
- IP адресов
- Протоколов

НО…приложения изменились

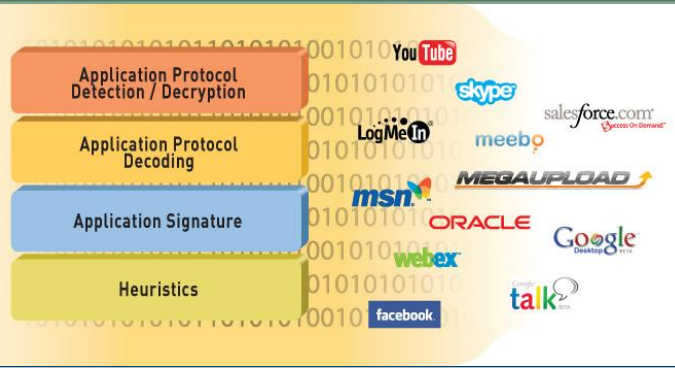
- Порты ≠ Приложения
- IP-адреса ≠ Пользователи
- Пакеты ≠ Контент



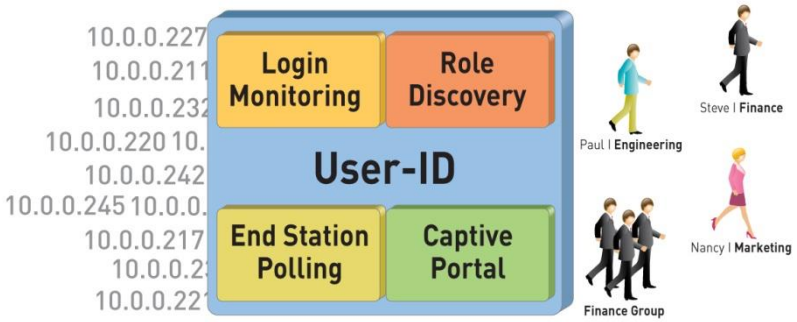
Новый межсетевой экран должен восстановить контроль

PAN: инновационные технологии

App-ID™
Идентификация приложений



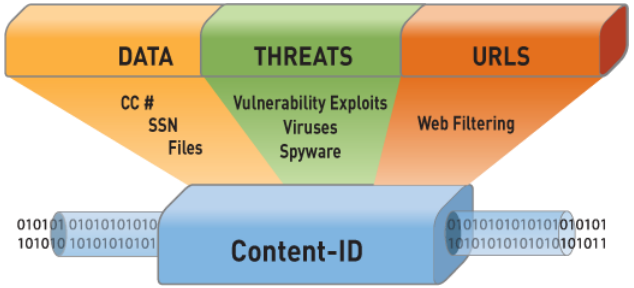
User-ID™
Идентификация пользователей



Content-ID™

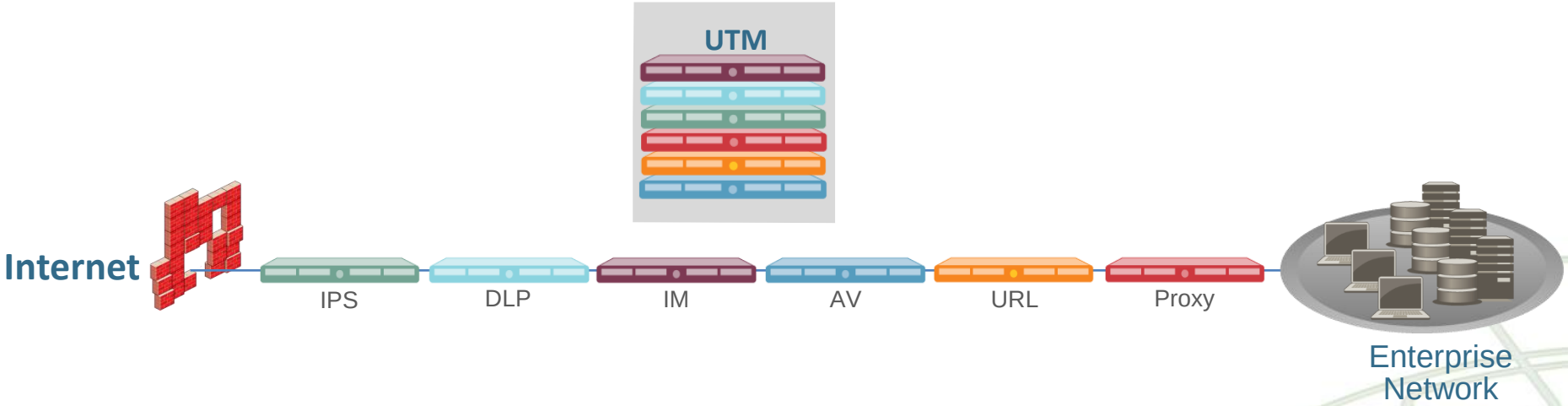
Контроль данных

+ SSL decryption



NGFW vs UTM

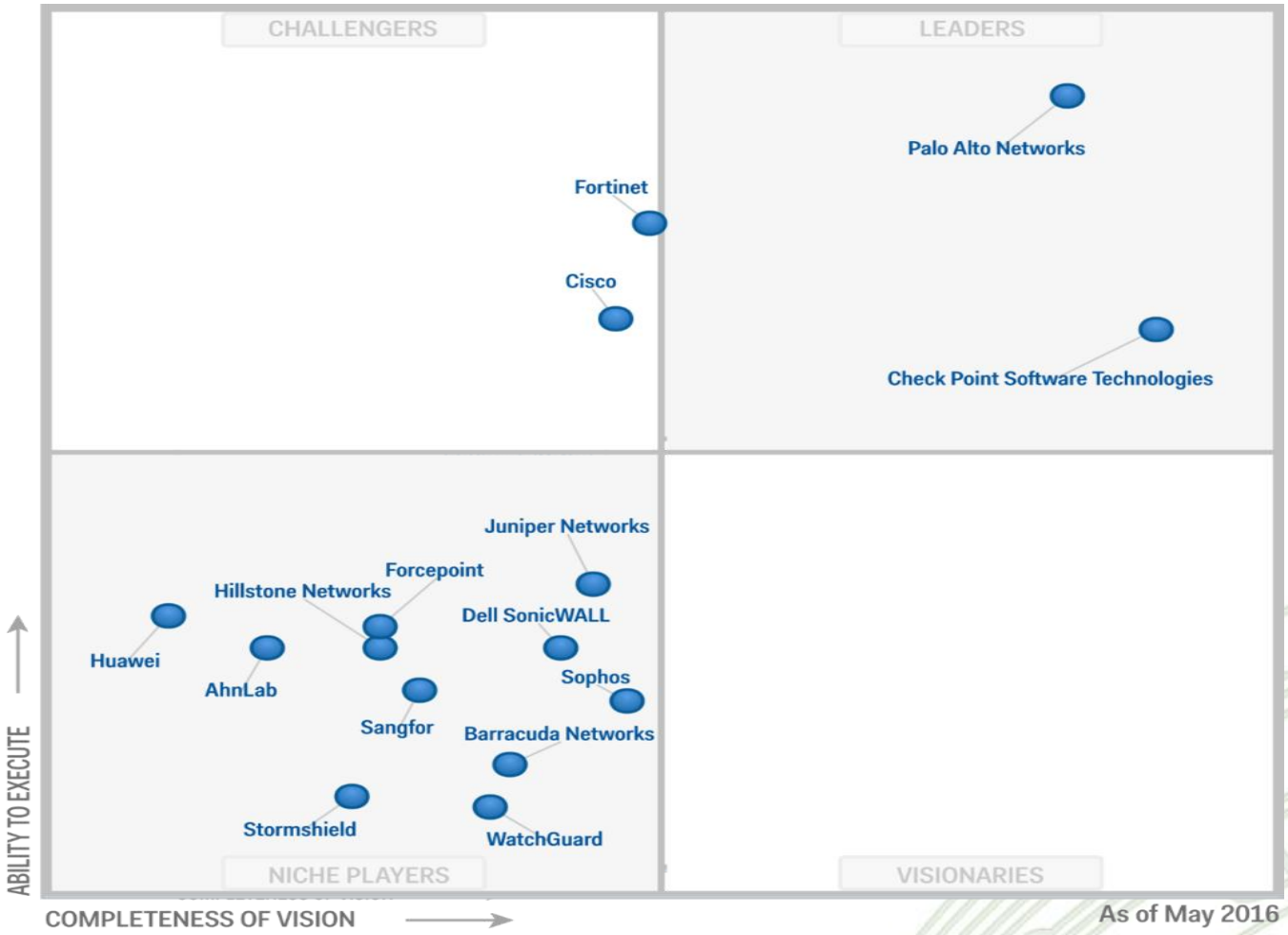
- Сложная топология и нет «прозрачной» интеграции
- «Помощники» межсетевого экрана не имеют полного представления о трафике – нет корреляции
- Дорогостоящее и дорогое в обслуживании решение



- Использование отдельных функциональных модулей в одном устройстве (UTM) делает его ОЧЕНЬ медленным

PAN: основные конкуренты

2015 Magic Quadrant for Enterprise Network Firewalls



PAN: линейка продуктов

PA-5060

20 Гбит/с FW/10 Гбит/с предотвращение атак/4,000,000 сессий

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit

PA-5050

10 Гбит/с FW/5 Гбит/с предотвращение атак /2,000,000 сессий

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit

PA-5020

5 Гбит/с FW/2 Гбит/с предотвращение атак /1,000,000 сессий

8 SFP, 12 RJ-45 gigabit

PA-3050

4 Gbps FW

2 Gbps threat prevention

500,000 sessions

12 copper gigabit

8 SFP interfaces

PA-3020

2 Gbps FW

1 Gbps threat prevention

250,000 sessions

12 copper gigabit

8 SFP interfaces

VM Series (VMware/Citrix SDX, Amazon)

До 1 Gbps FW

До 600 Mbps threat prevention

До 250,000 sessions

Гостевая машина или в режиме гипервизора

PA-500

250 Мбит/с FW/100 Мбит/с предотвращение атак /64,000 сессий

8 copper gigabit

PA-200

100 Мбит/с FW/50 Мбит/с предотвращение атак/64,000 сессий

4 copper gigabit

PAN: линейка продуктов

	PA-7050 NPC	PA-7050 System	PA-7080 System
NGFW (L3-L7) Gbps	20	**120**	**200**
Threat Prev. Gbps	10+	**60+**	**100+**
Матрица коммутации		1.2 Тбит	1.2 Тбит
Встроенная система логирования		4x1TB HDD = 2TB RAID1	4x1TB HDD = 2TB RAID1

Минимальная стоимость:

PA-7080 + поддержка = 302 500 $

PAN: лицензирование

Номер	Наименование	Описание
PAN-500-2GB	Palo Alto Networks PA-500 appliance 2GB Memory	Устройство (программно-аппаратный комплекс)
PAN-PA-500-TP	Threat prevention subscription year 1, PA-500	Лицензия на IPS/Антивирус/АнтиSpyware (ключ активации технической поддержки)
PAN-PA-500-URL4	PANDB URL filtering subscription year 1, PA-500	Лицензия на URL фильтрацию (ключ активации технической поддержки)
PAN-PA-500-WF	WildFire subscription year 1, PA-500	Лицензия на поведенческий антивирус (ключ активации технической поддержки)
PAN-PA-500-GP	GlobalProtect Gateway subscription year 1, PA-500	Лицензия на внутренний шлюз (ключ активации технической поддержки)
PAN-SVC-BKLN-500	Partner enabled premium support year 1, PA-500	Обновления и поддержка (ключ активации технической поддержки)

Threat Prevention (требуется лицензия)	
Потоковый антивирус (включая проверку HTML, Javascript, PDF и архивов), spyware, worms	☑
Drive-by download protection	☑
Обнаружение бот-сетей по поведению	☑
Modern Malware Protection (требуется лицензия WildFire)	
Обнаружение неизвестных вирусов в файлах по поведению, включая проверку неисполняемых документов PS, PDF, MS Office, Java, Android	☑
Автоматическое создание сигнатур для новых вирусов	☑
Контроль каналов управления бот сетей	☑
URL Filtering (требуется лицензия)	
Собственные категории URL	☑
Черные и белые списки	☑
Safe search (Google, Bing, Yahoo)	☑

Минимальная стоимость: PA-200 + поддержка = 3269 $

Поддержка – 1 год, 3 года, 5 лет

PAN: сертифицирование

PA-500/PA-5000 сертификат

РД «**Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля доступа отсутствия недекларированных возможностей**» по 4-ому уровню контроля и заданию по безопасности с оценочным уровнем доверия ОУД2 (усиленный) в соответствии с РД “Безопасность информационных технологий. Критерии оценки безопасности информационных технологий”, в том числе по 3-ему классу защищенности для межсетевых экранов

- “Требования к средствам антивирусной защиты”, Профиль защиты средств антивирусной защиты типа “Б” четвертого класса защиты;
- “Требования к системам обнаружения вторжений”, Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты;
- РД “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации” по 3-ему классу защищенности;
- РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля доступа отсутствия недекларированных возможностей» по 4-ому уровню контроля;

PAN: UTD

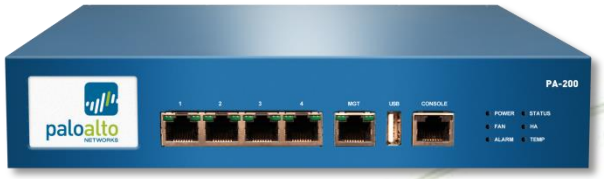
Участники семинара узнают, как важно блокировать любые известные и неизвестные угрозы и вирусы, а также привязывать кибер-атаки к определённым пользователям и устройствам для эффективной защиты ресурсов компании.

Основные темы семинара:

- 1 час - Презентация с рассказом о продукте который будет тестироваться
- 4 часа – Тест драйв устройств сетевой защиты NGFW и хостовой защиты TRAPS

Подробности семинара:

- Дата проведения – **октябрь 2016г.** для заказчиков
- Время проведения - с 10:00 до 14:00
- Место проведения - офис IT Guard, Москва
- Язык проведения мероприятия – русский
- Стоимость участия – бесплатно
- Аудитория – технические специалисты заказчиков
- Количество мест – строго 12



IT Guard

DISTRIBUTION OF LEADING INFORMATION
SECURITY TECHNOLOGIES

115093, Moscow, Partijny per., 1/46
Phone: +7 495 767-16-19